CMS

Illinois Department of

Central Management Services

State of Illinois

Certificate Policy for Digital Signature And Encryption Applications v1.7

August 25th, 2006

DOCUMENT VERSION CONTROL

VERSION	DATE	AUTHOR(S)	DESCRIPTION	REASON FOR CHANGE
0.1	19-Feb-00	Neal Fuerst	Initial draft	Initial Draft
0.2	10-May-00	Tait,Knox,Rosen	2nd draft	First State rework
0.3	12-0ct 00		3rd draft	Neil's comments
0.4	18-Oct-00	Anderson, Crossland, Hamby, Robinson, Tait	4th draft	Incorporate workgroup changes
1.0	14-Nov-00	Anderson, Crossland, Hamby, Robinson, Tait	Working policy for root key generation	Incorporate group changes
1.1	05-Sep-01	Anderson, Crossland, Hamby, Robinson, Tait	Final	FBCA changes, registration model update
1.2	25-OCT-01	Anderson, Crossland, Hamby, Robinson	Final	FBCA changes, key recovery & device certificate update
1.2.1	17-Dec-01	Anderson	Final	Title change, minor clarifications
1.2.2	19-Mar-02	Anderson	Final	Clarify sections 5.2.1, 5.2.3, 5.7,URL
1.2.3	24-July-02	Anderson	Final	Clarification of definitions; Correction to Executive Summary; Correction to sections 3.3.2, 4.1.1, 4.1.3; Web site added to section 4.2.1; typo corrected in 4.5.1; Paragraph

				moved from 4.7.1 to 4.7; Clarification made to 4.7.3; Paragraph removed from section 4.8.1; Clarification of revocation time added to section 5.5.3; Approved by Policy Authority 7/24/02.
1.2.3	13-Sept-02	Anderson	Second revision	Corrected section 4.1.4 to remove reference of being bound by the terms of the CPS. Corrected section 4.6.1 to remove reference to suspending certificates. Approved by Policy Authority as minimal impact on 09/20/02.
1.2.4	03-Jan-03	Anderson	Final	Corrected web addresses in sections 3.3.6.1 and 4.2.1. Added reference to out-of-state registration process in section 5.1.1. Miscellaneous page numbers were corrected in the table of

				contents.
1.2.4	24-Mar-03	Anderson	Final – after comment period	Changed zip code in section 3.4. Corrected upper and lower case on table of contents for section 9.
1.3	13-April-03	Wells, Anderson	Version for Review for Federal Bridge Mapping	Changes to complete Federal Bridge Mapping. Miscellaneous typing mistakes. Added the notification of all cross certified CA's in the event of CA private key update in 4.1.1. Added statement about using PKIX-CMP protocol when delivering the certificate in 5.3 Deleted wording about key validity period and inserted wording about prior to key expiration. Also deleted the wording on shared secrets provided at certificate application in 5.6.2. Deleted "rekey will" with

				“recovery after revocation will generally” and inserted wording on LRA’s may allow exceptions and the dot point about a user that is unable to present themselves and it is not a key compromise situation in 5.6.4. Inserted the word “secured” in front of shared secrets in 5.7.1. Replaced expired logs will be purged and destroyed with out of date logs will be purged after being archived in 5.8.2. Added the wording giving priority to certificate status during compromise or disaster recovery situations in 5.10 Added a paragraph about the exclusive use of all hardware and software to the CA’s operation and all the other services are to be turned off in

				6.1.1 Added continuous and documented to training requirements in 6.3.1 Connected the FIPS 140-1 level 3 to FIPS 140-1 level 1 to RA, LRA, and subscriber cryptographic module validation sin 7.3.1. Added dot points in 7.6 to make consistent with CPS 6.5 – Computer Security Controls.
1.3	Aug-19-2003	Anderson	Final	Updated section 4.1.1 to update language about 100% availability and to add maintenance down time.
1.4	Dec-1-2003	Anderson	Draft after Audit review	Updated web links in sections 3.3.6.1,4.2.1, and 4.7.6; Updated section 4.9 to update non-

				existent section 5.5.4.7. Approved by Policy Authority 02/26/04.
1.4	Apr-19-2004	Anderson	Final – after web comment period	No changes required.
1.4	May-11-2004	Anderson	1.4 draft	Updated section 6.3.2 to include the need of a signed LRA agreement and the acceptance of a background check less than 2 years old. Approved by Policy Authority May-26-2004 as minor changes with no version number increase.
1.4	Sep-24-2004	Anderson	1.4 draft	Updated section 3.4 to correct contact information; Updated section 5.7.2 and 5.7.3 to correct language on “involuntary recovery”. Approved by Policy Authority as minimal change requiring no version number update 09/29/2004.
1.5	April-6-2005	Anderson	Proposed – Before web comment period	Updated Section 4.2.1 to add language regarding authorizing an LRA to verify

				background checks for level-4 certificates. Approved by Policy Authority 03/30.2005.
1.5	July-13-2005	Anderson	Final after web comment period.	No changes recommended or received.
1.5	July-15-2005	Anderson	Proposed after audit recommendations	Changed wording in section 4.3.1; removed the word “substantially”. Changed wording in section 4.6 from “will” to “shall”. Changed wording in section 4.8.4 from “is” to “shall be”. Changed wording in section 4.9 from “grants” to “shall grant”.
1.5	July-21-2005	Anderson	Final	Approved by Policy Authority via email vote 07/20-21/2005.
1.6	Sep-15-2005	Anderson	Draft	Changed wording in section 4.3.1; replaced the word “substantially”.

				Section 4.8.1 was updated to reflect the safeguarding of any shared secret information. Section 5.5.3 was updated to indicate that revoked certificates are included on all new CRL publications until expiration. Section 5.8.1 was updated to indicate the use of logbooks and paper forms for certain audit information collection. Section 5.9.3 was updated to indicate that unauthorized users cannot modify archive files. Section 5.10 was updated to refer to the existing PKI disaster recovery document. Section 5.11 added to deal with multiple certificates due to different registration methods.

				Section 6.1.1 was updated to indicate the use of test systems and reference to the Root Key Generation ceremony as the basis of the secure environment.
1.6	Oct-5-2005	Anderson	Final	Approved by Policy Authority via email vote 09/27-29/2005.
1.6.1	Aug-09-2006	Anderson	Draft	Section 3.4 modified to change contact information; Section 4.1.4 was modified to remove the use of OCSP; Section 4.2.3 was modified to remove the word “repository”; Section 5.1.2 was modified to indicate that LRA’s can validate device certificate requests; Section 5.2.2 has been modified to correct the misuse of the term “RDN”, when the terms “cn”, and “DN” should be used; Section 5.6.3

				was modified to indicate that device certificates do automatically perform key-rollover and that re-validation of the certificate should take place at this time; Section 5.9.5 was modified to remove the word “correspondence”; Section 7.4.1 was modified to indicate that all CA keys will be retained in archive;
1.7	Aug-25-2006	Anderson	Final (version change from 1.6.1)	Approved by PA via email vote – 8/25/2006.

TABLE OF CONTENTS

1. DEFINITIONS

This list of definitions will evolve as the State PKI evolves. It will include formal definitions from other sources and informal definitions being used by the State.

Accreditation	Defined in ISO-IEC Guide 2 as a: "procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks." The accrediting body is a recognized entity which accredits the auditor as qualified to perform its evaluation of CAs or other PKI components, applying standards derived from the Certificate Policies adopted by the Policy-adopting body. Examples of bodies who have or might perform such a role include NIST's National Voluntary Laboratory Accreditation Program (NVLAP), or the American Institute of Certified Public Accounts (AICPA) which accredits Third Party Auditing Firms to audit various entities.
Activation Data	Private data, other than keys, that are required to access cryptographic modules.
Assurance Level	A representation of how rigorously the Registration Authority authenticates the identity claimed by an Applicant prior to issuing a Certificate.
Authority Revocation List (ARL)	A list of revoked Certificate Authority Certificates. An ARL is a Certificate Revocation List for Certificate Authority certificates.
Authentication	The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Audit	An Independent review and examination of documentation, records and activities to access the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.
Certificate	A Certificate issued under this Policy by a Certificate Authority and identified as such by the inclusion of the registered object identifier for this Certificate Policy in the *Certificate Policies* field, and at a minimum: • Identifies the Certificate Authority issuing it. • Names or otherwise identifies its Subscriber. • Contains a public key that corresponds to a private key under the control of the Authorized Subscriber. • Identifies its operational period.

	• Contains a Certificate serial number and is digitally signed by the Certificate Authority issuing it. The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.
Certificate Authority (CA)	A Certificate Authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. A Certificate Authority can perform the functions of a Registration Authority (RA) and can delegate or outsource this function to separate entities. A Certificate Authority performs two essential functions. First, it is responsible for identifying and authenticating the intended Authorized Subscriber to be named in a Certificate, and verifying that such Authorized Subscriber possesses the private key that corresponds to the public key that will be listed in the Certificate. Second, the Certificate Authority actually creates and digitally signs the Authorized Subscriber's Certificate. The Certificate issued by the Certificate Authority then represents that CA's statement as to the identity of the person named in the Certificate and the binding of that person to a particular public-private key pair.
Certificate Extension	A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.
Certificate Manufacturing	The process of accepting a public key and identifying information from an authorized Subscriber, producing a digital certificate containing that and other pertinent information, and digitally signing the Certificate.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements. For example, a particular Certificate Policy might indicate applicability of a type of Certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
Certificate Authority Software	The application software required to manufacture certificates by the CA
Certification Practice Statement (CPS)	A statement of the practices, which a CA employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the CA uses to satisfy the requirements specified in the CP that are supported by it.
Certificate Revocation List (CRL)	A list of revoked Certificates that is created, time stamped and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases,

	the CA may choose to split a CRL into a series of smaller CRLs. When an End Entity chooses to accept a certificate the Relying Party Agreement requires that this Relying Party check that the certificate is not listed on the most recently issued CRL.
Cross-Certificate	A Certificate used to establish a trust relationship between two Certification Authorities. A Cross-Certificate is a Certificate issued by one CA to another CA which contains a CA key associated with the private CA signature key used for issuing Certificates. Typically a cross-certificate is used to allow End Entities in one CA to communicate security with End Entities in another CA. A cross-certificate issued by CA#1 to CA#2 allows Entity #a, who has a Certificate issued by CA#1, to accept a Certificate used by Entity #b, who has a Certificate issued by CA#2.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine: • Whether the transformation was created using the private signing key that corresponds to the signer's public verification key. • Whether the message has been altered since the transformation was made.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the End Entity within the CA domain.
Encryption Key Pair	A public and private key pair issued for the purposes of encrypting and decrypting data.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
End Entity	A person, device or application that uses the keys and Certificates created within the PKI for purposes other than the management of the aforementioned keys and Certificates. An End Entity may have the roles of a Subscriber or a Relying Party.
Entity	Any autonomous element within the PKI. This may be a CA, a RA or an End Entity.
Employee	An employee is any person employed in or by the State; as well as contractors and other persons who have been authorized to access electronic networks.
Federal Information	Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software,

Processing Standards (FIPS)	data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.
Governing Body	Authorities that dictate Policy and procedures that may impact the Policy Authority and Operational Authority.
Hardware Token	A hardware device that can hold private keys, digital certificates, or other electronic information that can be used for authentication or authorization. Smartcards and USB tokens are examples of hardware tokens.
Internet Engineering Task Force(IETF)	The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Issuing CA	In the context of a particular Certificate, the issuing Certificate Authority is the Certificate Authority that signed and issued the Certificate.
Key Generation	The process of creating a Private Key and Public Key pair.
Key Pair	Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the public key, it is computationally infeasible to discover the other key which is called the private key.
Local Registration Authority (LRA)	An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (i.e., an LRA is delegated certain tasks on behalf of a RA or CA).
Object Identifier (OID)	An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognized standards organization.
Operational Authority (OA)	An agent of the State PKI CA. The **Operational Authority** is responsible to the **Policy Authority** for: • Interpreting the *Certificate Policies* that were selected or defined by the **Policy Authority**. • Developing a *Certification Practice Statement (CPS),* in accordance with the *Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 2527)*, to document the CA's compliance with the Certificate Policies and other requirements.

	• Maintaining the CPS to ensure that it is updated as required. • Operating the Certificate Authority in accordance with the CPS.
Operational Period of a Certificate	The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or is earlier revoked.
Organization	Department, agency, partnership, trust, joint venture or other association.
PKIX	A set of IETF Working Group developed technical specifications for PKI components based on X.509 Version 3 Certificates.
Person	A human being (natural person), corporation, limited liability company, or other judicial entity, or a digital device under the control of another person.
PIN	Personal Identification Number. See activation data for definition
Policy	This Certificate Policy.
Policy Authority (PA)	An agent of the Certificate Authority. The **Policy Authority** is responsible for: • Dispute resolution. • Selecting and/or defining *Certificate Policies*, in accordance with the *Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 2527)*, for use in the Certificate Authority PKI or organizational enterprise. • Approving of any interoperability agreements with external Certificate Authorities. • Approving practices, which the Certificate Authority must follow by reviewing the *Certification Practice Statement* to ensure consistency with the *Certificate Policies.* • Providing Policy direction to the CA and the **Operational Authority**.
Public Key Infrastructure (PKI)	A structure of hardware, software, people, processes and policies that uses Digital Signature technology to provide Relying Parties with a verifiable association between the public component of an asymmetric key pair with a specific Subscriber.
Private Key	The private key of a key pair used to perform public key cryptography. This key must be kept secret.

Public Key	The public key of a key pair used to perform public key cryptography. The public key is made freely available to anyone who requires it. The public key is usually provided via a Certificate issued by a Certificate Authority and is often obtained by accessing a repository.
Public/Private Key Pair	Two mathematically related keys, having the properties that: • One key can be used to encrypt a message that can only be decrypted using the other key. • Even knowing the public key, it is computationally infeasible to discover the private key.
Registration	The process whereby a user applies to the Certification Authority for a digital certificate and the CA issues a Certificate for that user.
Registration Authority (RA)	An Entity that is responsible for the identification and authentication of Certificate Subscribers before Certificate issuance, but does not actually sign or issue the Certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party	A **Relying Party** is a recipient of a Certificate signed by the State PKI CA who acts in reliance on those Certificates and/or digital signatures verified using that Certificate and who has agreed to be bound by the terms of this CP and the CPS.
Relying Party Agreement	An agreement subscribed to by a recipient of a Certificate signed by the State PKI CA prior to gaining access to any State PKI CA CRL.
Repository	The logical single Repository operated for all Subscribers and Relying Parties on the Network. All Certificates issued by all CAs, and all Certificate Revocation Lists relating thereto, shall be published in the Repository. Also known as a “Directory”.
Revocation	To prematurely end the operational period of a Certificate from a specified time forward.
Root CA	The CA that issues Certificates to each CA operating under this Policy.
Security Accreditation Authority	An agent of the CA. Responsible for: • Approving the operation of the CA in a particular mode using particular safeguards. • Accepting residual security risks on behalf of the CA domain or enterprise.
Signature Key Pair	A pubic and private key pair used for the purposes of digitally signing electronic documents and verifying digital signatures.

Software-based Certificate	A digital certificate (and associated private keys) that are created and stored in software – either on a local workstation or on a secure server.
Sponsoring Organization	An organization with which an Authorized Subscriber is affiliated (e.g., as an employee, user of a service, business partner, customer etc.).
Subscriber	An entity that is the subject of a Certificate and which is capable of using, and is authorized to use, the private key, that corresponds to the public key in the Certificate. Responsibilities and obligations of the **Subscriber** shall be as required by the *Certificate Policy*.
Token	A hardware security device containing an End Entity's Private Key(s) and Public Key Certificate. (see "Hardware Token")
Trustworthy System	Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.
Valid Certificate	A Certificate that (1) a Certificate Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not "valid" until it is both issued by a CA and has been accepted by the Subscriber.

2. EXECUTIVE SUMMARY

Section 2 Executive Summary is intended to be a layman's description of the State of Illinois Public Key Infrastructure. This section is not intended to describe the policies and procedures that govern the PKI. Policies and procedures are described in the Sections 3 through 9 of this document and those sections govern all PKI operations.

The State of Illinois has created a Public Key Infrastructure (PKI) to facilitate development of electronic applications that could replace many of the paper processes currently employed by the State's agencies. This document and the associated Certification Practice Statement describe the policies and procedures that govern operation of the State of Illinois PKI. The PKI provides tools that can identify users to an electronic application, that can help enforce or apply confidentiality and privacy requirements, and that provide electronic signatures that comply with both the federal E-Sign act and the State of Illinois' Electronic Commerce Security Act (5 ILCS 175).

A Public Key Infrastructure includes many participating entities. The Certification Authority (CA) for the State of Illinois PKI is operated by the Department of Central Management Services. Policies and procedures for the PKI are developed and approved by the Policy Authority (PA) which includes representatives from several State agencies. Subscribers are individuals who register and are issued digital certificates. A Relying Party is an entity that uses the digital certificates as part of an electronic process.

Public Key Infrastructure uses the technology of public key encryption to provide functionality to users and applications. Users (whether individuals, electronic applications, or devices) are registered and two encryption keys are created – one held privately by the user and one made publicly available. The keys are mathematically related in that each operates as the inverse of the other, however the value of one key cannot be determined by analyzing the other. The public key is also contained in the digital certificate which is issued to the user by the CA. This digital certificate contains information which identifies the user to the CA and links the user's keys to that identity. The State of Illinois PKI operates using a model commonly referred to as a "dual key pair" in which registered users are issued one digital certificate consisting of a corresponding public/private key pair for encryption and a second corresponding public/private key pair for signature purposes. Data that is encrypted using a given public key can only be decrypted using the corresponding private key. Likewise, a digital signature created using a given private key can only be verified by using the corresponding public key.

Digital certificates that are issued by the CA are identified according to how rigorously the user is authenticated during the registration process. This identification is called the assurance level and can be used to determine whether a certificate can be relied on as part of a given process. High risk or highly sensitive transactions typically require a higher assurance level while a lower level of assurance may suffice for more mundane processes.

Subsequent sections of this document describe requirements, obligations, and procedures for each participant in the PKI. More detailed and specific descriptions of the procedures are included in the associated Certification Practice Statement.

3. INTRODUCTION

3.1 PURPOSE

This document defines all certificate policies of the Certificate Authority (“CA”) operated by The State of Illinois (“State”) for the use of digital certificates for encryption and digital signatures for use in providing electronic identification of End-Entities as required for conducting State business. Unless specifically noted in this document by the inclusion of unique requirements for each individual policy, the requirements of this document apply to all certificates issued by this CA.

This policy defines a single private Public Key Infrastructure consisting of the Certificate Authority, at least one Registration Authority, Local Registration Authorities, and End-Entities.

This Policy is for use by all entities with relationships with the CA, including End-Entities, Registration Authorities (“RA”) and Local Registration Authorities (“LRA”) and other cross-certified CAs undertaking to adhere to this Policy.

This Policy is binding on the CA, and governs its performance with respect to all Certificates it issues. Specific practices and procedures by which the CA implements the requirements of this Policy are maintained in a Certification Practice Statement (“CPS”) that is approved by the State Policy Authority (“PA”).

3.2 POLICY IDENTIFICATION

This document is called the State of Illinois Certificate Policy for Digital Signature and Encryption Applications (CP).

The CA issues certificates for use in verification of digital signatures and certificates for use in encryption. The CA supports several certificate policies that cover both of these applications.

Each policy is uniquely represented by an “object identifier” which is a numeric string that is contained in a field of each certificate issued by the CA under this CP. To ensure interoperability and uniqueness of this Object Identifier (“OID”), The State has registered this OID following the procedures specified in ISO/IEC and ITU standards.

The Object Identifiers for this CA’s policies are:

Authentication Level	Object Identifier
Level I (software-based)	2.16.840.114273.1.1.1.1
Level I (hardware token)	2.16.840.114273.1.1.1.2
Level II (software-based)	2.16.840.114273.1.1.1.3
Level II (hardware token)	2.16.840.114273.1.1.1.4
Level III (software-based)	2.16.840.114273.1.1.1.5
Level III (hardware token)	2.16.840.114273.1.1.1.6
Level IV (hardware token only)	2.16.840.114273.1.1.1.7
MEDI Single-Use	2.16.840.114273.1.1.2.1

The procedures for implementing this policy are described in the State of Illinois Certification Practice Statement.

3.3 ROLE IDENTIFICATION

3.3.1 Certificate Authority ("CA")

- Creates, signs, distributes and revokes Certificates binding the *X.500 Distinguished Name* of Subscribers and Registration Authorities with their respective signature verification key and their public encryption key;
- Publishes certificate status through certificate revocation lists (CRLs);
- Has designed, implemented, and operated its Certification Practice to reasonably achieve the requirements of this Policy.

The CA may use one or more representatives or agents to perform its obligations under this Policy, provided that the CA remains responsible for complying with this Policy.

Where necessary, this Policy distinguishes the different users and roles accessing the CA functions. Where this distinction is not required, the term CA shall refer to the total CA entity, including the software and its operations.

The CA may issue cross-certificates to other CAs where expressly authorized by the Policy Authority. Cross-certificates will be issued to other CAs where a cross-certification agreement has been developed between the PA and the policy governing body of the other CA. Cross-certification will be implemented according to the requirements defined in that agreement.

3.3.2 Policy Authority ("PA")

The Policy Authority ("PA") is responsible for ensuring that both the policy and the practices that the CA employs in issuing certificates, as may be more comprehensively described in the CPS, are consistent with the policies described in this CP.

The PA shall consist of individuals representing constitutional offices, state agencies, and local governments which are utilizing the State of Illinois public key infrastructure.

3.3.3 Operational Authority ("OA")

The Illinois Department of Central Management Services shall serve as the Operational Authority (OA). The Operational Authority ("OA") is responsible for the operation of the CA in accordance with this CP and the practices described in the CPS.

The State Operational Authority ("OA") shall make a copy of this CP available to all End-Entities within its CA.

3.3.4 Registration Authorities ("RA")

At least one RA will be appointed by the State PA and will be responsible for the identification and authentication of End-Entities in accordance with this CP.

3.3.5 Local Registration Authorities ("LRA")

Each State Agency participating in the State PKI, and other entities as determined by the PA, may appoint one or more LRAs to be responsible for the identification and authentication of End-Entities within the Agency organization and its constituency in accordance with this CP.

3.3.6 End Entities

End-Entities in this PKI may include State employees, individuals conducting electronic business with the State, hardware devices and/or specific applications. At the discretion of the PA, any person entity, hardware device or specific application may be a Subscriber or Relying Party (collectively referred to as an "**End Entity**") in the State PKI. End-Entities may also use Certificates issued by the CA to encrypt information for, and verify the digital signatures of, other End-Entities within the State PKI.

3.3.6.1 Subscribers

This CP shall be binding on each Subscriber that applies for and/or obtains Certificates, by virtue of the Subscriber Agreement**,** and governs each applicant's performance with respect to their application for, use of, and reliance on, Certificates issued by the CA. The Subscriber agreement may be viewed at http://www.illinois.gov/pki/pki_subscriber.cfm.

3.3.6.2 Relying Parties

Any entity that has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them, and which has agreed to be bound by the terms of this CP and the CPS.

By accepting a certificate issued pursuant to the provisions of this CP, a relying party agrees to be bound by the provisions of this CP. The following factors, among others are significant in evaluating the reasonableness of a recipient's reliance upon a certificate, and upon digital signatures verifiable with reference to the public key listed in the certificate:

(1) Facts which the relying party knows or of which the relying party has notice, including all facts listed in the certificate or incorporated in it by reference;

(2) The value or importance of the digitally signed message, if known;

(3) The course of dealing between the relying person and the subscriber, and the available indicia of reliability or unreliability apart from the digital signature;

(4) The usage of trade, particularly trade conducted by trustworthy systems or other computer based means.

3.4 CONTACT DETAILS

This Certificate Policy is administered by the PA.

Inquiries, suggested changes, or notices regarding this Certificate Policy should be directed to:

Val Falzone

State of Illinois PKI Policy Authority Chairperson

1021 North Grand Ave. East

Springfield, IL 62794

Val.Falzone@epa.state.il.us

Telephone: 217-785-1605

4. GENERAL PROVISIONS

4.1 OBLIGATIONS

4.1.1 CA Obligations

The CA shall:

- Provide CA services with a maximum available application target of 100% and allowing for normal maintenance, and in accordance with the policies and processes described in this Certificate Policy and the Certification Practice Statement. In the event of a major disaster, service could be interrupted.
- Issue certificates to Subscribers, in accordance with the certificate policies referenced herein as well as the procedures and practices described in the Certification Practice Statement;
- Revoke certificates which are issued by this CA, upon receipt of a valid request to do so from either the subscriber who is the subject of the certificate to be revoked, an RA, LRA or the CA itself, as required by the Certificate Policy;
- Issue and publish CRLs on a regular schedule as required by the Certificate Policy;
- Notify Subscribers that certificates have been issued to them or that their certificate has been revoked; and
- Notify others (e.g. Relying Parties) of certificate issuance/revocation by provision of access to certificates, CRLs in the State PKI repository.
- Securely notify all cross-certified CA's of CA private key update.

4.1.2 RA and LRA Obligations

The RA or LRA shall verify the accuracy and authenticity of the information provided by Subscribers to the RA or LRA at the time of application for a certificate. Pursuant to the terms of a valid Subscriber Agreement, the RA or LRA may make use of the State employment records to verify the data by comparing the application information with information in the State databases. The RA shall provide this verification on behalf of the CA.

Each LRA shall verify the accuracy and authenticity of the information provided by the Subscribers to the LRA at the time of application for a certificate. The CA may, but is not required to, verify the accuracy and authenticity of information provided by Subscribers through an LRA.

When an agency or entity is implementing level-4 (biometric) certificates, the Policy Authority may authorize a trusted individual within the agency or entity to validate the background checks received before the level-4 certificate is created. This individual should possess a level-3 certificate, and must be a Local Registration Authority (LRA).

4.1.3 Subscriber Obligations

Subscribers shall:

- Make true representation at all times to the CA, the RA and the appropriate LRAs regarding information in their certificates; and other identification and authentication information;
- Use certificates in a manner consistent with this Certificate Policy;
- Take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of their private keys;
- Protect their Certificate user password;
- Upon issuance of a Certificate naming the applicant as the Subscriber, review the Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the Certificate;
- Inform the RA or appropriate LRA within 48 hours of a change to any information included in their certificate or certificate application request;
- Inform the RA or appropriate LRA within 8 hours of a suspected compromise of one/both of their private keys; and
- Rightfully hold private keys corresponding to the public keys listed in their certificate.

4.1.4 Relying Party Obligations

End entities that rely on Certificates shall:

- Verify that the State issued certificate is within the validity period specified within the certificate;
- Verify certificates through appropriate means including a) revocation status checking through use of Certificate Revocation Lists (CRLs).
- Trust and make use of certificates only if the validity of the certificate is established between the relying party and the certificate subject. and
- Relying parties shall rely on a valid Certificate for purposes of verifying the digital signature only if prior to reliance, the Relying Party shall:

  (1) Agreed to be bound by the terms of this CP;

(2) Verified the digital signature by reference to the public key in the Certificate; and

(3) Referred to the most recent CRL.

Relying party understands that certificates are subject to revocation and such action will not be reflected in the Certificate itself, but must be verified by consulting the most recent certificate revocation list.

4.2 PUBLICATION AND REPOSITORIES

4.2.1 Publication of CA Information

This CP shall be published electronically and can be located at http://www.illinois.gov/pki.

The following PKI information shall be published in the State Directory:

- All encryption and signing public key certificates issued by the CA to digital certificate users;
- All revocations of digital certificate user public key certificates performed by the CA;
- All revocations of cross-certification certificates issued by the CA.

4.2.2 Frequency of Publication

Certificates shall be published in the Directory immediately as they are issued.

CRLs shall be published in the Directory as they are issued (following the timeline described in Section 5.5.4).

4.2.3 Access Controls

The State of Illinois Operational Authority shall protect any information not intended for public dissemination or modification. Public keys and certificate status information in the State of Illinois repository shall be publicly available through the Internet. The use of certificates to access information in Agency repositories shall be determined by the Agency pursuant to its authorizing and controlling statutes.

4.2.4 Repositories

The repository for this CA is provided by an *X.500 directory system. The Lightweight Directory Access Protocol* (LDAP) version 2 or higher protocol shall be used to access the Directory.

4.3 LIABILITIES

As the CA and RA functions are provided by the State, the liability issues related to both functions are combined in this CP.

Nothing in this Certificate Policy shall create, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on the State by virtue of any contract or obligation that is otherwise determined by applicable law.

The State shall have no liability to any subscriber, relying party and any other entity for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to use of a Certificate or any services provided by the State. Use of any Certificate is limited by the terms of this CP and the CPS. This CP also contains limited warranties and disclaimers of representations, warranties and conditions.

4.3.1 Disclaimers

Provided that the State has substantially complied with the certificate policy, and the certificate practices statement, the State shall not be liable for any loss which:

(1) Is incurred by the subscriber of a certificate issued by the State, or any other person, or

(2) Is caused by reliance upon a certificate issued by the State, upon a digital signature verifiable with reference to a public key listed in a certificate, or upon information represented in such certificate, or repository.

In addition to the foregoing, the State specifically disclaims liability for loss or damages:

- Incurred between the time a certificate is revoked and the next scheduled issuance of a CRL;
- Due to unauthorized use of certificates issued by the CA, and use of certificates beyond the prescribed use defined by the Certificate Policy under which the certificate was issued;
- Caused by fraudulent or negligent use of certificates and/or CRLs issued by the CA;
- Due to disclosure of personal information contained within certificates and revocation lists;
- Due to erroneous authentication of user identity; and,
- Due to losses incurred if not notified of revoked certificates.

The State makes no representations and gives no warranties or conditions, whether express, implied, statutory, by usage of trade, or otherwise and the State specifically disclaims any and all representations, warranties and conditions of merchantability, non-infringement of copyright or patent rights of others, title, satisfactory equality, or fitness for a particular purpose.

4.3.2 Loss Limitations

In no event shall the State or any State employee, Director or Agent, incur any liability arising out of or relating to any digital certificate or any services provided by the State in respect to Certificates whether issued by the State of Illinois CA or another. This limitation shall apply regardless of the number of transactions, digital signatures, or causes of action arising out of related to such Certificate or any services provided regarding any such Certificate. The foregoing limitations shall apply to any claim whatsoever, whether based in contract, tort, or any other theory of liability and shall be applicable to subscribers, relying parties and any other person relying upon, issuing, or applying for a Certificate from the State of Illinois or any other CA under this Certificate Policy.

In no event shall the State, or any State employee, Director, or Agent be liable for any incidental, special, punitive, exemplary, indirect, reliance, or consequential damages (including without limitation, damages for loss of business, loss of business opportunities, loss of good will, loss of profits, business interruption, loss of data, lost savings or other similar losses) whether arising out of theories of contract, tort, or any other theory of liability.

4.3.3 Other Exclusions

Without limitation, the State shall not be liable to any Subscribers, Relying Parties, other CAs, or any other person, entity or organization for any losses, costs, expenses, liabilities, damages, claims or settlement amounts arising out of or relating to use of a Certificate or any services provided by the State in respect to the Certificates if:

- The Certificate was issued as a result of errors, misrepresentations, or other acts or omissions of a Subscriber or of any other person, entity, or organization;

- The Certificate has expired or has been revoked;

- The Certificate has been modified or otherwise altered;

- The Subscriber has violated the Certificate Policy, Certification Practice Statement, or its Subscription Agreement or a Relying Party is in violation of the Certificate Policy, Certification Practice Statement or its Relying Party Agreement;

- The Private Key associated with the Certificate has been compromised; or

- The Certificate is used other than as permitted by this Certificate Policy and the associated Certification Practice Statement or is used in contravention of applicable law.

In no event shall the State be liable for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising out of or relating to its refusal to issue a Certificate.

In no event shall the State be liable to any Subscriber, Relying Party, other CA, or any other person, entity, or organization for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to any proceeding or allegation that a Certificate or any contents of a Certificate infringe, misappropriate, dilute, unfairly compete with, or otherwise violate any patent, trademark, copyright, trade secret, or any other intellectual property right or other right of any person, entity, or organization in any jurisdiction.

4.3.4 Hazardous Activities

The Certificates and the services provided by the State under this Certificate Policy and the associated Certificate Practice Statement are not designed, manufactured or intended for use in or in conjunction with hazardous activities or uses requiring fail-safe performance, including but not limited to the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control, medical devices or direct life support machines. The State specifically disclaims any and all representations and warranties with respect to such hazardous activities or uses, whether express, implied, statutory, by usage of trade, or otherwise.

4.4 FINANCIAL RESPONSIBILITY

Subscribers and Relying Parties shall be responsible for the financial consequences to such Subscribers and Relying Parties relating to any transactions in which such Subscribers or Relying Parties participate and which use the Certificates or any services provided by the State in relation to the Certificates. The State makes no representations and gives no warranties and conditions regarding the financial efficacy of any transaction completed utilizing a Certificate or any services provided by the State in relation to the Certificates and the State shall have no liability except as explicitly set forth herein in respect to the use of or reliance on a Certificate or any services provided by the State in relation to the Certificates.

4.4.1 Hold Harmless: Relying Parties

Relying parties shall hold the State harmless from and against any and all liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney’s fees, court costs and experts fees) arising out of or relating to (i) any use or reliance by a relying party on the Certificate or any service or transaction provided by the State or performed by a relying party in connection with the Certificates, (ii) lack of proper validation of a CA certificate by a relying party, (iii) reliance by the relying party on an expired or revoked the Certificate, (iv) use of a Certificate other than as permitted by the State Certificate Policy, Certification Practice Statement , the subscription agreement, any relying party agreement, and applicable law, (v) failure by a relying party to exercise reasonable judgment in the circumstances in relying on a Certificate, or (vi) any claim or allegation that the reliance by a relying party on a Certificate or the contents of a Certificate infringes, misappropriates, dilutes, unfairly competes with, or otherwise violates the rights (including intellectual property rights) of any third party in any jurisdiction. Notwithstanding the foregoing, Relying Parties shall not be obligated to hold the State harmless in respect to any liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to any willful misconduct by the State.

4.4.2 Hold Harmless: Subscribers

Subscriber shall hold the State harmless from and against any and all liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to (i) any use or reliance by the subscriber on any Certificate or any service or transaction provided by the State or performed by the subscriber in connection with the Certificates, (ii) any misrepresentation made by subscriber in using or applying for a Certificate, (iii) modification made by subscriber to the contents of a Certificate, (iv) use of a Certificate other than as permitted by the State Certificate Policy, Certification Practice Statement, the subscription agreement, any relying party agreement, and applicable law, (v) loss, disclosure, compromise or unauthorized use of the private key corresponding to the public key in subscriber's the Certificate, or (vi) any allegation that the use of a subscriber's the Certificate or the contents of a subscriber's the Certificate infringes, misappropriates, dilutes, unfairly competes with, or otherwise violates the rights (including intellectual property rights) of any third party in any jurisdiction. Notwithstanding the foregoing, a subscriber shall not be obligated to hold the State harmless in respect to any liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to any willful misconduct by the State.

4.4.3 Fiduciary Relationships

Nothing contained in the State Certificate Policy, Certification Practice Statement or in any Subscription Agreement, or any Relying Party Agreement shall be deemed to constitute either the State, or any of its subcontractors, agents, suppliers, employees, or directors the partner, agent, trustee, or legal representative of any Subscriber, Relying Party or any other third party or to create any fiduciary relationship between the State and any Subscriber, Relying Party or any other third party, for any purpose whatsoever. Nothing in this CP, or in any Subscription Agreement or any Relying Party Agreement shall confer on any Subscriber, Relying Party, or any other third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the State.

4.5 INTERPRETATION AND ENFORCEMENT

4.5.1 Governing Law

The laws of the State of Illinois, excluding its conflict of laws, rules and any applicable treaties, shall govern the construction, validity, interpretation, enforceability and performance of this CP, all Subscription Agreements and all Relying Party Agreements. Any dispute in respect to this CP, any Subscription Agreement, any Relying Party Agreement, or in respect to the Certificates or any services provided by the State in respect to the Certificates, shall be brought in the Illinois Court of Claims, and each person, entity, or organization hereby agrees that such courts shall have personal and exclusive jurisdiction over such disputes.

4.5.2 Force Majeure

The State shall not be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or comply with the terms of this CP, any Subscription Agreement, or any or settlement amounts arising out of or related to delays in performance or from failure to perform Relying Party Agreement due to any causes beyond its reasonable control, which causes include, without limitation, acts of God, so-called "hackers," "crackers" or other computer intruders, or the public enemy, riots and insurrections, acts of terrorism, war, accidents, fire, strikes and other labor difficulties, embargoes, judicial action, lack of or inability to obtain export permits or approvals, necessary labor, materials, energy, utilities, components or machinery, acts of civil or military authorities.

4.5.3 Interpretation

All references in this CP to “Sections” refer to the sections of this CP. As used in this CP, neutral pronouns and any variations thereof shall be deemed to include the feminine and masculine and all terms used in the singular shall be deemed to include the plural, and vice versa, as the context may require. The words “hereof,” “herein” and “hereunder” and other words of similar import refer to this CP as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this CP. The words "include" and “including” when used herein is not intended to be exclusive and mean, respectively, "include, without limitation," and “including, without limitation.”

4.5.4 Severability, Survival, Merger, Notice

4.5.4.1 Severability

Whenever possible, each provision of this CP, any Subscription Agreements, and any Relying Party Agreements shall be interpreted in such manner as to be effective and valid under applicable law. If the application of any provision of this CP, any Subscription Agreements, or any Relying Party Agreements or any portion thereof to any particular facts or circumstances shall be held to be invalid or unenforceable by a court of competent jurisdiction, then (i) the validity and enforceability of such provision as applied to any other particular facts or circumstances and the validity of other provisions of this CP, any Subscription Agreements, or any Relying Party Agreements shall not in any way be affected or impaired thereby, and (ii) such provision shall be enforced to the maximum extent possible so as to effect its intent and it shall be reformed without further action to the extent necessary to make such provision valid and enforceable.

For greater certainty, it is expressly understood and agreed that every provision of this CP, any subscription agreements, or any relying party agreements that deal with (i) limitation of liability or damages, or (ii) disclaimers of representations, warranties, conditions, or liabilities, is expressly intended to be severable from any other provisions of this CP, any subscription agreements, or any relying party agreements and shall be so interpreted and enforced.

4.5.4.2 Survival

Sections 4.2 (Publication and Repositories), 4.3 (Liabilities), 4.4 (Financial Responsibility), 4.5 (Governing Law), 4.8 (Confidentiality), 4.9 (Intellectual Property Rights), 5.4 Certificate Acceptance), 5.5 (Certificate Suspension and Revocation), 9. (Policy Administration) shall survive termination or expiration of this CP, any Subscription Agreements, and any Relying Party Agreements. All references to sections which survive termination of this CP, any Subscription Agreements, and any Relying Party Agreements, shall include all subsections beneath such Section. All payment obligations shall survive any termination or expiration of this CP, any Subscription Agreements, and any Relying Party Agreements.

4.5.4.3 Merger

This CP, the CPS, all Subscription and Relying Party Agreements state all of the rights and obligations of the State and any Subscriber or Relying Party in respect to the subject matter hereof and thereof and such rights and obligations shall not be augmented or derogated by any prior agreements, communications or understandings of any nature whatsoever whether oral or written. The rights and obligations of the State may not be modified or waived orally and may be modified only in a writing signed or authenticated by a duly authorized representative the State.

4.5.4.4 Conflict of Provisions

In the event of a conflict between the provisions of this CP and the CPS, and any express written agreement between the State and a Subscriber or Relying Party, with respect to a Certificate or any services provided by the State with respect to the Certificates, the terms described in the CP and the CPS shall take precedence. In the event of a conflict between the provisions of this CP and CPS and a cross-certification agreement executed between the PA and the entity responsible for another CA, the terms of the cross-certification agreement shall take precedence.

4.5.4.5 Waiver

The failure of the State to enforce at any time any of the provisions of this CP, the CPS, a Subscription Agreement, or a Relying Party Agreement or the failure to require at any time performance by any other party of any of the provisions of this CP, the CPS, a Subscription Agreement, or a Relying Party Agreement shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of the State to enforce each and every such provision thereafter. The express waiver by the State of any provision, condition, or requirement of this CP, the CPS, a Subscription Agreement, or a Relying Party Agreement shall not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

4.5.4.6 Notice

Any notice to be given by a Subscriber, or Relying Party under this CP, the CPS, a Subscription Agreement, or a Relying Party Agreement shall be given in writing to the address specified below by prepaid receipted mail, facsimile, or overnight courier, and shall be effective as follows (i) in the case of facsimile or courier, on the next Business Day, and (ii) in the case of receipted mail, five (5) Business Days following the date of deposit in the mail. Any notice to be given by the State under this CP, the CPS, any Subscription Agreement, or any Relying Party Agreement shall be given by email or to the last address for the Subscriber on file with the State. In the event of notice by email, the notice shall become effective on the next Business Day. In the event of notice to the last address on file with the State, notice shall become effective as specified in (i) or (ii), depending on the means of notice utilized.

Notice address for the State:

State of Illinois Digital Certificate Authority

Department of Central Management Services

201 W. Adams

Springfield Illinois 62704-1874

4.5.4.7 <u>Assignment</u>

The Certificates and the rights granted under this CP, the CPS, any Subscription Agreement, or any Relying Party Agreement are personal to the Subscriber to whom a Certificate was issued, and to the person, entity, or organization which entered into the Subscription Agreement or Relying Party Agreement with the State, and cannot be assigned, sold, transferred, or otherwise disposed of, whether voluntarily, involuntarily, by operation of law, or otherwise, without the prior written consent of the State. Any attempted assignment or transfer without such consent shall be void and shall automatically terminate such Subscriber's or Relying Party's rights under this CP, the CPS, any Subscription Agreement, or any Relying Party Agreement.

The State may assign, sell, transfer, or otherwise dispose of this CP, any Subscription Agreement, or any Relying Party Agreement together with all of its rights and obligations under this CP, the CPS, any Subscription Agreements, and any Relying Party Agreements (i) to an affiliate, or (ii) as part of a sale, merger, or other transfer of all or substantially all the assets of the business of the State to which this CP, the Subscription Agreements, and Relying Party Agreements relate. Subject to the foregoing limits, this Agreement shall be binding upon and shall inure to the benefit of permitted successors and assigns of the State, Subscribers, and Relying Parties, as the case may be.

4.5.5 <u>Dispute Resolution Procedures</u>

Within the CA domain, disputes between Certificate users, one of which acts in the role of a subscriber and the other which acts in the role of a relying party, or between Certificate users and the CA or the RA, will initially be reported to the PA for resolution. Such reports should be sent in writing to the address listed in 4.5.4.6.

4.5.6 Limitation Period

Any and all legal actions in respect to a dispute which is related to a Certificate or any services provided in respect to a Certificate shall be commenced prior to the end of one (1) year after (i) the expiration or revocation of the Certificate in dispute, or (ii) the date of provision of the disputed service or services in respect to the Certificate, whichever is sooner. If any action in respect to a dispute which is related to a Certificate or any service or services provided in respect to a Certificate is not commenced prior such time, any party seeking to institute such action shall be barred from commencing or proceeding with such action.

4.6 FEES

No direct fees shall be assessed by the CA or OA.

In cross-certification agreements with business partner organizations, the costs are expected to balance naturally between the State and the business partner organization. Any exceptions, which may result in additional fees for any of the services outlined in this section and its subsections, will be addressed in the specific cross-certification agreement itself and are outside the scope of this CP.

4.6.1 Certificate Issuance, Renewal, Suspension, and Revocation Fees

The CA will issue, renew, and revoke Subscribers certificates at no cost.

4.6.2 Certificate Access Fees

The CA shall not impose any certificate access fees on Subscribers with respect to its own Certificate(s) or the status of such Certificate(s).

4.6.3 Certificate Validation Services Fees

The State shall not impose fees for certificate validation services.

4.6.4 Fees for Other Services such as Policy Information

The CA shall not impose fees for access to policy information.

4.6.5 Refund Policy

Because no fees shall be charged for certificate services, as specified in this CP, there is no need to provide for refunds.

4.7 COMPLIANCE AUDIT

The purpose of such audit shall be to verify that the Certificate Authority has a system in place to attest to the quality of the Certificate Authority Services that it provides and to ensure that this system complies with the requirements of this CP and the associated CPS.

4.7.1 Frequency of Certificate Authority Compliance Review

The CA shall undergo a compliance audit prior to initial approval as a CA to demonstrate compliance with State Policies and this CP and the CPS. Subsequent compliance audits shall be required every twelve months, or whenever substantive changes are made to the CP or the CPS.

The auditing of the Root Key Generation Ceremony will be considered the initial audit for the purposes of this Certificate Policy.

Subsequent audits shall be conducted either by an independent auditor contracted by the Department of Central Management Services, or in conjunction with the annual IT compliance audit of the Department of Central Management Services Bureau of Communication & Computer Services.

4.7.2 Qualifications of Auditor

Annual audits are performed by independent auditors selected by the State of Illinois. Auditors must demonstrate competence in the field of compliance audits and must regularly perform such compliance audits as a primary responsibility.

4.7.3 Auditor's Relationship to Audited Party

Annual audits shall be performed either by third party independent auditors contracted specifically for the purpose of auditing the State’s PKI operations, or by auditors employed by the State of Illinois who are independent of the OA or PA.

4.7.4 Topics Covered by Audit

The annual audit investigates the operations of the CA and RA functions of the State PKI to ensure their compliance with this CP and the CPS. Some areas of focus for these audits are:

- **Identification & Authentication**

  Initial Registration

  Routine Rekey

  Rekey after Revocation

  Revocation Request

- **Operational Requirements**

  Certificate Application

  Certificate Issuance

  Certificate Acceptance

  Key Recovery

  Certificate Suspension/Revocation

  Computer Security Audit Procedures

  Records Archival

  CA key Changeover

  Compromise and Disaster Recovery

  CA Termination

- **Physical, Procedural & Personnel Security**

  Physical Security Controls

  Procedural Controls

  Personnel Security Controls

- **Technical Security Controls**

  Key Pair Generation & Installation

  Private Key Protection

  Other Aspects of Key Pair Management

  Activation Data

  Computer Security Controls

  Lifecycle Security Controls

  Network Security Controls

  Cryptographic Module Engineering Controls

- **Certificate & CRL Profiles**

  Certificate Profile

CRL Profile

- **Specification Administration**

  Contact Information

  Specification Change Procedures

  Publication and Notification Procedures

  Approval Procedures

4.7.5 Actions Taken as a Result of Deficiency

If a deficiency is identified by the auditor, the State PA will, based upon the findings of the auditor, determine which of the following actions will be taken:

a.) Continue to operate as usual;

b.) Continue to operate but with limitations on rights; or

c.) Suspend operation

If action a) or b) is taken the State PA and OA are responsible for ensuring that corrective actions are taken within a reasonable time frame. At that time, or earlier if agreed by the PA and auditor, the audit team will reassess. If, upon reassessment, corrective actions have not been taken, the PA will determine if more severe action (e.g. action c) above) is required.

If action c) is taken all certificates issued by the CA, including end-user certificates, are revoked prior to suspension of the service. The State PA and OA are responsible for reporting the status of corrective action to the auditors on a weekly basis. The PA and auditor together will determine when the re-assessment is to occur. Upon reassessment, if the deficiencies are deemed to have been corrected, the CA will resume service and new certificates will be issued to Certificate users.

4.7.6 Communication of Results

Results of the annual audit are provided to the State PA, The State of Illinois Department of Central Management Services’ Chief Security Officer, as well as the Auditor General. The State PA with input from the auditor will determine if Certificate users need to be informed of any action as a result of the audit. The State PA will communicate to Certificate users via the internet at http://www.illinois.gov/pki.

4.8 CONFIDENTIALITY

4.8.1 Types of Information to be kept confidential

The Subscriber's private signing key must be kept confidential by the Subscriber. The CA and RA are not provided any access to those keys.

The Subscriber's private encryption key must be kept confidential by the Subscriber; however, the CA may recover private encryption keys for State of Illinois employees as described in Section 5.7 Key Recovery.

Personal information held by the CA , other than that which is explicitly published as part of a certificate, CRL, certificate policy, or this document is considered confidential and shall not be released unless required by law.

Shared secret information shall be either encrypted, hashed, stored securely, or otherwise physically protected.

In addition, personal information submitted to the CA by Subscribers:

- Must be made available to the subscriber for individual review following an authenticated request by said subscriber;
- Must be subject to correction and/or update by said subscriber;
- Must be protected by the CA in such a way as to insure the integrity of said personal information.

4.8.2 <u>Disclosure of information considered confidential</u>

The CA, RA, or any LRA shall not disclose certificate or certificate-related information to any third party except when:

- authorized to do so by this CP.
- required to be disclosed by law or court order
- authorized to do so by the certificate holder

Any requests for disclosure of information must be signed and submitted to the CA. The CA shall communicate all such requests to the PA.

4.8.3 <u>Types of information not considered confidential</u>

Information included in public certificates and CRLs issued by the CA are not considered confidential.

Information in this Certificate Policy is not considered confidential.

4.8.4 <u>Disclosure of certificate revocation information</u>

When a certificate is revoked by the CA, a revocation reason shall be included in the CRL entry for the revoked certificate. This revocation reason code is not confidential and may be shared with all users and Relying Parties. However, no other details concerning the revocation may be disclosed.

4.9 INTELLECTUAL PROPERTY RIGHTS

Certificates and CRLs issued by the CA are the property of the State.

This CP is the property of the State.

The Distinguished Names (DNs) used to represent entities within the CA domain in the Directory and in certificates issued to End-Entities within that domain, all include a relative distinguished names (RDN) for the State and as such are the property of the State.

With respect to the CA system, the Software, including any related copyright, trademark, and patent rights, is owned by Entrust Technologies and will remain the sole and exclusive property of Entrust Technologies.

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in a Certificate.

The State OIDs are the property of the State , which may be used only by the CAs in accordance with the provisions of this Policy. Any other use of the above without the express written permission of the State is expressly prohibited.

The State retains all of its right, title, and interest (including all intellectual property rights), in, to and under all the Certificates, except for any information which is supplied by a Subscriber and which is included in a Certificate, which shall remain the property of the Subscriber. All Subscribers grant to the State a non-exclusive, worldwide, paid-up, royalty-free license to use, copy, modify, publicly display, and distribute such information, by any and all means and through any and all media whether now known or hereafter devised for the purposes contemplated under this CP, the Subscriber’s Subscription Agreement, and any Relying Party Agreements. The State shall be entitled to transfer, convey, or assign this license in conjunction with any transfer, conveyance, or assignment by the State as contemplated in Section 4.5.4.7. The State grants to Subscribers and Relying Parties a non-exclusive, non-transferable right to use, copy, and distribute the Certificates, subject to such Certificates being used as contemplated under the State Certificate Policy, the CPS, the Subscriber’s Subscription Agreement, and any Relying Party Agreements, and further provided that such the Certificates are reproduced fully and accurately and are not published in any publicly available database, repository or Directory without the express written permission of the State.

The State shall grant permission to reproduce this CP provided that (i) the copyright notice on the first page of this CP is retained on any copies of this CP, and (ii) this CP is reproduced fully and accurately. The State retains all right, title, and interest, in, to and under this CP, including all intellectual property rights therein.

In no event shall the State be liable to any Subscribers or Relying Parties or any other third parties for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising from or relating to claims of infringement, misappropriation, dilution, unfair competition, or any other violation of any patent, trademark, copyright, trade secret, or any other intellectual property or other right arising from or relating to the use of the Certificate or in the use of any services provided by the State in relation to any Certificate.

5. OPERATIONAL REQUIREMENTS

This section describes operational requirements imposed by this Policy on the CA, RAs, LRAs and End Entities. It includes handling of Certificate revocations, audit logs, and transaction archives.

5.1 CERTIFICATE APPLICATION

5.1.1 Application for a Certificate by an Individual

The RA and appropriate LRAs will accept certificate applications from state employees or individuals who need to conduct electronic business with the State of Illinois through three primary means: web, in-person and bulk applications.

Web registration is available for users of Agency-based web applications. The registration process is handled entirely through the internet, with the applicant providing necessary identification information on a web form. The RA validates the identity information provided by the applicant against one or more trusted data sources.

A web registration process is available for out-of-state residents who desire a State of Illinois digital certificate. This process instructs the recipient to download a form, take it to a notary public, present proper identification, and have the form notarized. This form is then mailed to the OA, where activation codes are created and distributed to the recipient in a secure manner. These codes are then entered into a secure web page to generate the certificate. All out-of-state certificates are created as a level 1 certificate as described in section 5.2.3.

In person applications may be accepted by the RA or any authorized LRA. The applicant must submit a completed State of Illinois Digital Certificate Application in person at the time of application.

Bulk applications for state agency staff or other definable groups of individuals will be accepted by the RA from appropriate LRAs in accordance with procedures developed on a case by case basis. These procedures will comply with all requirements of this Certificate Policy and will be issued at the assurance level determined from evaluating the authentication provided by the bulk registration process using the authentication requirements described in Section 5.2.3.

For each Certificate application, prospective Subscribers will satisfy the following requirements:

- Provide proof of identity as required in Section 5.2.3
- Submit a completed State of Illinois Digital Certificate Application to the RA or appropriate LRA;
- Indicate agreement with the terms and conditions for use of the State’s public key infrastructure as described in the Subscriber’s Agreement;
- Initialize the client software on their workstation (if appropriate); and,

- Demonstrate to the RA that the private keys have been successfully installed.

5.1.2 Application on behalf of A Device Or Software Application Or Process

The RA will accept certificate applications submitted on behalf of hardware devices and software applications or processes that are owned by the State of Illinois or operated by an external entity for the purpose of inter-operating with or operating on behalf of the State. Applications will be accepted from State employees or LRAs holding currently valid Certificates issued by this CA and shall be signed by the appropriate LRA or the agency Director, if no agency LRA is available. The application must include appropriate identification information for the device, a description of the device, the name of the person responsible for maintaining the device, and the purpose that the certificate will serve if issued. For certificates issued to external entities, the application must also include the name of the State agency employee who is responsible for the ongoing relationship with the external entity which requires the certificate.

5.1.3 Application for a cross-certificate

The PA will develop the necessary procedures to apply for a cross-certificate.

An application for a cross-certificate does not obligate the PA to authorize a cross-certificate. The PA will review any CA’s request for cross-certification and approve or deny the request according to established procedures.

A CA requesting cross-certification will include with application:

- Its Certificate Policy
- An external audit report validating the assurance level stated in the CP
- The public verification key generated by the CA
- A statement describing how the proposed cross-certification will benefit the State of Illinois and its citizens

5.2 INITIAL REGISTRATION

5.2.1 Types of Names

Each End Entity must have a clearly distinguishable and unique X.500 Distinguished Name (DN) in the Certificate subject name field in accordance with IETF RFC 2459.

This Policy does not allow for the utilization of pseudonymous names in certificates.

5.2.2 Name Composition

The common name (cn) will be a combination of first name(s) and surname. Middle initials and other identifiers may also be used.

The DN must be unique for all End Entities of the CA. For each End Entity additional numbers or letters may be appended to ensure the DN's uniqueness.

In the case of device entities, the DN will include a meaningful description of the device in addition to another form of distinguishable information such as the DN for the individual administering the device.

Decisions regarding DN composition and resolution of any disputes regarding name composition or name forms will be made by the PA.

5.2.3 Identification and Authentication of Individual

An application for an individual to be a Subscriber may be made by the individual or by another person or organization authorized to act on behalf of the prospective Subscriber.

Identification and authentication of the prospective Subscriber must be in accordance with the procedures specified in the State Certification Practice Statement.

The RA or LRA shall keep a record of the type and details of the identification used.

Assurance Level	Identification Requirements
Level I	Identity may be established by comparison of user supplied identity information with a trusted information source; or by attestation of an LRA or other Trusted Agent.
Level II	Identity shall be established by in-person proofing before an RA, an LRA, or other Trusted Agent. User shall produce two credentials, one of which must be a Secretary of State photo I.D.
Level III	Identity shall be established by in-person proofing before an RA, an LRA, or other Trusted Agent. User shall produce two credentials, one of which must be a Secretary of State photo I.D. Approval subject to completion of a background check.
Level IV	Identity shall be established by in-person proofing before an RA, an LRA, or other Trusted Agent. User shall produce two credentials, one of which must be a Secretary of State photo I.D. Approval subject to completion of a background check. Private keys shall be secured using a biometric device

5.2.4 Identification and Authentication of Device or Software Application

An application for a device or a software application to be a Subscriber may be sponsored by an individual who represents the organization that is accountable for the device or application. The RA or LRA must authenticate and register the individual as part of the process of authenticating the device or application. Both the authentication of the sponsoring individual and the authentication of the device or application shall follow the procedures described in this CP and the corresponding CPS.

5.3 CERTIFICATE ISSUANCE

The issuance and publication of a Certificate by the CA indicates a complete and final approval of the certificate application by the CA. A self-signed root CA certificate is securely delivered to the subscriber using PKIX-CMP protocol during the certificate issuance process.

5.4 CERTIFICATE ACCEPTANCE

As part of the certificate issuance process, a Subscriber will explicitly indicate acceptance or rejection of the Certificates to the CA and will expressly acknowledge to the RA or LRA prior to delivery that it will adhere to this Policy, both as Subscriber and as Relying Party.

As part of the certificate verification process, a Relying Party must agree to be bound by the terms of the Relying Party Agreement, and must expressly acknowledge and accept the terms of the same prior to being afforded access to any certificate validity information.

5.5 CERTIFICATE REVOCATION

5.5.1 Revocation Request

Revocation of an Individual’s certificate may be requested by the CA, the LRA for the Subscriber’s organization, a State agency, or by the Subscriber.

Revocation of a certificate issued to a device or application may be requested by the individual who sponsored the application for the certificate or another individual authenticated as representing the organization accountable for the device or application.

RA and LRAs will permit Subscribers to request revocation of a Certificate in which the requestor is identified as the Subject in the certificate. RA and LRAs will adhere to the procedures identified in the State CPS for authentication of revocation requests.

5.5.2 Circumstances for Revocation

A Certificate will be revoked when the Subscriber no longer wants or requires a certificate, or when the Public Key password, token or profile associated with the certificate is compromised or suspected of being compromised. Certificates may also be revoked by the CA upon failure of the Subscriber to meet its obligations under this Policy or any other agreement, regulation, or law that may be in force. Subscribers shall request revocation promptly following detection or suspicion of a compromise or any other event necessitating revocation. The RA or LRA may originate a certificate revocation if knowledge or suspicion of compromise is obtained. The rationale for such a revocation will be documented, signed by at least one of the CA personnel, and archived.

A Certificate holder's encryption and/or verification certificate is revoked when the certificates are no longer trusted, for any reason. Some of the specific reasons for loss of trust in certificates include, but are not limited to:

- Compromise or suspected compromise of private keys and/or user passwords and profile;
- Failure of the subscriber to meet their obligations under this CP and CPS;
- Failure to prove continued ownership of the private keys;
- Request by the Subscriber;
- Receipt of a certified copy of subscriber's death certificate;
- When information on a certificate changes or becomes obsolete; or
- If the issuing CA determines that the Certificate was not properly issued in accordance with the Certificate Policy.

Agency staff may see indications that a particular certificate cannot be trusted through the course of conducting electronic transactions that involve a particular certificate; however, change in employment status with the agency is NOT by itself a justification for revocation of a certificate.

5.5.3 Procedure for Revocation

In the event a revocation request is initiated by an entity other than the Subscriber, the Subscriber shall be afforded reasonable notice and opportunity for hearing. Where the risk to the security and integrity of a private key suggest a reasonable likelihood of irreparable harm absent immediate revocation, a certificate may be revoked without prior notice and opportunity for hearing, provided the subscriber is afforded reasonable notice and opportunity for hearing following Certificate revocation.

A revocation request may be generated electronically. The request will be signed with the Subscriber's private signing key and sent to the RA or LRA. Alternatively, the Subscriber may notify the RA or LRA in writing.

All revocation requests and the resulting actions taken by the RA or LRA will be archived.

The CA notifies Relying Parties by posting revoked certificates to a CRL in the public Directory. Revocation shall be effective upon publication of the CRL.

Revoked certificates shall be included on all new publications of the CRL until the certificates expire.

5.5.4 Time to Process Revocation Request and CRL Frequency

Revocation requests will be processed within 18 hours from time of receipt by the RA. CRLs will be published upon revocation of a Certificate or at least every 24 hours.

5.5.5 Certificate Suspension

Not supported.

5.5.6 CRL Checking Requirements

Certificates may be stored locally in the Relying Party's Public Key application but, before use, the status of the certificate will be checked against a CRL less than twenty-four (24) hours old. When a Relying Party downloads a CRL from the Directory, the Relying Party will verify the CRL by checking its digital signature.

5.6 KEY CHANGEOVER

5.6.1 Automatic Rekey

The RA sets keys for automatic renewal/update as required. Revoked or expired Certificates shall not be renewed.

5.6.2 Routine Rekey - Individual

Routine rekey occurs prior to key expiration as described in 7.4.1 Validity Periods for Public and Private Keys. Subscribers may update certificates automatically unless the certificate has been revoked or previously updated – except that the Subscriber's identity must be re-established through the existing registration process at least once every nine years. For automatic update the subscriber will be authenticated through the current private signature key. Any time that automatic rekey is blocked, the Subscriber's identity must be re-established through the existing registration process.

5.6.3 Routine Rekey – Device or Application

Certificates issued to devices and applications shall be automatically renewed when the key validity period expires. The device or application and its sponsoring organization and individual shall be re-evaluated at the time of rekey.

5.6.4 Rekey After Revocation

For Subscribers whose Certificates have been revoked, recovery after revocation will generally not be permitted until the Subscriber's identity is re-established through the existing registration process. LRA's may allow exceptions in the following situation:

- An Entrust user is temporarily unable to present themselves in person (e.g. on extended travel) and the revocation was not due to a key compromise.

5.7 KEY RECOVERY

The CA does not escrow or archive Subscriber's private keys; however, the Subscriber's profile can be recovered, creating a new set of keys and a new password that controls access to those keys. This process can only be completed by three different CA personnel and shall only occur under one of the following three circumstances:

5.7.1 Recovery at Subscriber Request

A Subscriber may request that the Subscriber's own profile be recovered if the Subscriber is no longer able to access his/her private keys because the password has been lost or the electronic file has been corrupted. The Subscriber must provide proof of identity through secured shared secrets or other authentication prior to recovery of the Subscriber's profile.

5.7.2 Involuntary Recovery at State Agency Request

- A State Agency may request involuntary recovery of a Subscriber's private encryption keys if that person is or has recently been employed by the State of Illinois, the Agency has reason to believe that data necessary to agency operations has been encrypted using the Subscriber's keys, and the Agency is unable to contact the Subscriber or the Subscriber is unable or unwilling to decrypt the data.

- The Agency's request shall be made in writing to the PA, describing why the Subscriber's private encryption key is necessary to Agency operations and specifying what use will be made of the key. The request shall be signed by the Director of the Agency. The Subscriber's keys shall not be recovered until said request is reviewed by the PA or those designated by the PA to review such requests.

- Prior to recovering the Subscriber's profile, the CA shall alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate shall be recovered and the profile will be delivered to the Agency LRA on physical media. The LRA shall sign for receipt of the profile, shall supervise all Agency use of the recovered key for the purposes described in the approved request and shall certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate shall be revoked following the procedures in Section 5.5 "Certificate Revocation".

- A Subscriber who's profile has been revoked as part of an involuntary recovery must follow the procedures described in Section 5.6.4 Rekey After Revocation to be re-authenticated and issued a new Certificate.

5.7.3 Involuntary Recovery by Court Order

- The PA and OA will comply with court orders to recover a Subscriber's keys.

- Prior to recovering the Subscriber's profile, the CA shall alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate shall be recovered and the profile will be delivered to the Agency LRA on physical media. The LRA shall sign for receipt of the profile, shall supervise all Agency use of the recovered key for the purposes described in the approved request and shall certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate shall be revoked following the procedures in Section 5.5 "Certificate Revocation".

- A Subscriber who's profile has been revoked as part of an involuntary recovery must follow the procedures described in Section 5.6.4 Rekey After Revocation to be re-authenticated and issued a new Certificate.

5.8 AUDIT LOGS

5.8.1 Types of Events Recorded

All significant events will be recorded in the CA audit logs in accordance with the procedures specified in the CPS. Logbooks, paper forms, and other physical mechanisms are used where automated collection of events is not possible.

5.8.2 Audit Log Processing

Audit logs will be reviewed at least once every week in accordance with the procedures specified by the CPS. Identified issues will be investigated and processed and out of date logs will be purged after being archived.

5.8.3 Retention Period for Audit Logs

Audit logs will be retained and archived in accordance with the procedures specified in the CPS.

5.8.4 Protection of Audit Logs

Access to audit logs will be protected by a combination of physical and logical security controls in accordance with the procedures specified in the CPS.

5.8.5 Audit Logs Backup

Audit log files will be backed-up and the backup media will be stored locally. A consolidated copy of the audit log files will be sent to a secure off-site storage facility in accordance with procedures specified in the CPS.

5.8.6 Notification Following a Critical Event

The CA and the Registration Authority application will notify the CA personnel of any critical security error or discrepancy as it is logged in accordance with procedures specified in the CPS.

5.9 RECORDS ARCHIVE

5.9.1 Types of Records Archived

The CA will archive all sensitive events, lists, certificates, keys, records, reports, agreements and correspondence in accordance with the procedures specified in the CPS.

5.9.2 Retention Period for Archive

All sensitive events, lists, certificates, keys, records, reports, agreements and correspondence archived shall be retained in accordance with the procedures specified in the CPS.

5.9.3 Protection of Archive

The archive media will be protected either by physical security, or a combination of physical security and cryptographic protection. Additionally, the archive media will be provided adequate protection from environmental threats such as temperature, humidity, and magnetism. No unauthorized user shall be permitted to write to, modify, or delete the archive.

5.9.4 Archive Backup Procedures

Certificates, CRLs, and keys will be backed-up and stored locally. A copy of these items will be made and sent to a secure archive facility in accordance with the procedures specified in the CPS.

For discrepancy and compromise reports, cross-certification agreements, and correspondence, a copy of the document shall be made as it is received and sent to a secure archive facility. Original copies shall be kept locally.

5.9.5 Archived Records and Archive Collection Systems

All sensitive events, lists, certificates, keys, records, reports, and agreements will be archived according to the procedures specified in the CPS.

Archived records will be transferred to separate physical media external to the CA host system and CA application.

5.10 COMPROMISE AND DISASTER RECOVERY

Compromise procedures and a Disaster Recovery Plan for the CA, RA and LRAs are in place in accordance with the procedures specified by the CA, giving priority to certificate status information. These procedures can be found in the document entitled “State of Illinois Central Management Services Public Key Infrastructure Recovery Activation Plan”.

5.11 MULTIPLE CERTIFICATES CAUSED BY DIFFERENT REGISTRATION METHODS

Due to differences between the original certificate creation method and the web registration model, some recipients have received multiple certificates (i.e., same common name with a different serial number). This generally occurred when someone had undergone a face-to-face registration and activation codes have been generated, but the recipient never activated their certificate. This situation is handled as stipulated in section 4.11 of the CPS.

6. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

This section outlines the physical, procedural, and personnel security controls required of the CA, RA, LRA and Subscribers to protect their operations.

6.1 PHYSICAL SECURITY CONTROLS

Physical security controls will be implemented to control access to the CA hardware and software. This includes the CA host computer and any external cryptographic hardware module or token.

6.1.1 Physical Security Controls for Certificate Authority

When the PKI system was first installed, the entire procedure was audited, videotaped, and scripted in the Root Key Generation Ceremony script. During this ceremony, software versions were examined and verified, hardware platforms were validated, and the entire environment was scrutinized to ensure integrity. This was the basis of the establishment of the secure environment. All future updates/changes to the environment are done in accordance with the CPS.

The CA host computer will be in a secure space with access control and CCTV systems. Access to the CA host computer will be limited to those personnel performing one of the roles described in this Policy. Access will be controlled through the use of electronic access controls, mechanical combination locksets, or deadbolts. The secure space will be monitored in accordance with procedures outlined in the CPS.

The CA hardware and software shall be dedicated to performing one task : the CA. There shall be no other applications; hardware devices, network connections, or component software installed which is not part of the CA operation. Any network ports or services that are not necessary to the operation of the CA services are disabled. The CA software verifies configuration via check-sum upon start-up to detect unauthorized modification to the CA software or configuration. Configuration changes are documented in audit logs. A formal configuration methodology shall be used for installation and ongoing maintenance of the CA system.

CA access control records will be maintained and audited periodically. Maintenance and service personnel will be escorted and supervised according to procedures outlined in the CPS.

All updates to the Certificate Authority and Master Directory computers shall first be applied and tested on test platforms before being applied to the production computers. Proper change management procedures shall be followed when updating the production systems.

6.1.2 Physical Security Controls for Registration Authorities

The RA and LRAs will implement at a minimum the following controls:

- The RA computers will have the boot-lock feature turned on and enable the password protected screen saver feature, and computers shall not be left unattended when the Private Key is in the unlocked state (i.e. when the password has been entered);
- The RA and LRA will physically protect any password that allows access to keys. Passwords should be memorized and not written down. If a password must be written down, it will be stored in a locked file cabinet or container accessible only to the RA or LRA;
- If a private key is stored encrypted on a diskette or other unsecured medium, such diskette or other medium will be stored in a locked file cabinet or container when not in use; and
- LRAs shall not leave their computers unattended when the Private Key is in an unlocked state (i.e., when the password has been entered).
- Any RA or LRA computer that contains private keys encrypted on a hard drive must be secured.

6.1.3 Physical Security Controls for Subscribers

Each Subscriber shall physically protect any password that allows entry into the Subscriber’s CA Client application. Passwords should be memorized and not written down. If a password must be written down, it shall be securely stored such that only the Subscriber has access to it. Subscribers shall not leave their computers unattended when the Private Key is in an unlocked state (i.e., when the password has been entered).

6.2 PROCEDURAL CONTROLS

Responsibilities at the CA host computer may be shared by multiple individuals assigned to multiple roles. Each account on the CA host computer and/or within the CA application should have limited capabilities commensurate with the role of the account holder. Two or more persons are required to perform the following tasks:

- Adding and deleting Security Administrators.
- Changing the Security Administrator’s password.
- CA Master Key updates.

A single person may be assigned to perform all LRA tasks.

6.3 PERSONNEL SECURITY CONTROLS

6.3.1 Personnel Security Controls for Certification Authorities

All system administrators required for on-site support during the in-service phase of the CA will be escorted.

CA and RA personnel will:

- Be appointed by the PA;
- Receive proper and continuous training in relation to their assigned duties (All training is documented.
- Be an employee or other authorized individual not subject to frequent re-assignment or extended periods of absence.

6.3.2 Personnel Security Controls for Local Registration Authorities

Each participating State agency, and other entities as determined by the PA, may nominate one or more individuals to serve as LRAs for the organization. Prospective LRA's will return a completed LRA application form and a signed LRA agreement (wet signature or digitally signed) to the RA and will submit themselves to a State Police criminal background check. If the background check reveals that the applicant has been convicted of or committed a crime of moral turpitude the application is subject to disqualification at the discretion of the PA. If an LRA is formally accused of a crime other than a petty traffic offense (for which the fine does not exceed $100.) he/she must within 3 days of being charged notify the CA who shall notify the PA.

A previously conducted background check will be accepted as long as it is no more than 2 years old at the time of applying to become an LRA.

6.3.3 Personnel Security Controls for Subscribers and Relying parties

Subscribers and Relying Parties will be made aware of any security practices they need to follow in the protection of their computers and cryptographic devices. The LRA is responsible for communicating these practices to all Subscribers and Relying Parties within its domain.

7. TECHNICAL SECURITY CONTROLS

The Client system and data will be secured in accordance with the policies described herein.

7.1 KEY PAIR GENERATION

All End Entities will be issued dual key pairs with separate keys for authentication/signing & confidentiality/encryption.

Each End Entity must generate its own signature key pair.   Signature keys for Level I, II & III certificates may be generated in hardware or software. For each level of assurance the Certificate OID shall identify whether the private key was generated in hardware or software.

The encryption key pair is generated by the CA and transmitted to the End Entity during the PKIX protocol session.

Level of Assurance	Key Generation Medium
Level I	Software – Desktop or Repository
	Hardware token
Level II	Software – Desktop or Repository
	Hardware token
Level III	Software – Desktop or Repository
	Hardware token
Level IV	Hardware token only

7.2 KEY SIZES

All signature key pairs generated within the CA will be at least 1024 bit RSA or, where the DSS is used, as stipulated in FIPS PUB 186.

7.3 PRIVATE KEY PROTECTION

7.3.1 Standards for Cryptographic Module

CA cryptographic operations will be performed by either hardware or software cryptographic module rated to at least FIPS 140-1 Level 3.

RA and LRA cryptographic operations shall be performed by either hardware or software cryptographic module validated to at least FIPS 140-1 Level 1.

Subscriber cryptographic operations will be performed by either hardware or software cryptographic module validated to at least FIPS 140-1 Level 1.

The modules need not necessarily operate in the FIPS mode.

7.3.2 Private Key Multi-Person Control

The simultaneous intervention of two or more persons is required for operations on the CA's private signing key as referred to in section 6.2 of this policy.

7.3.3 Private Key Backup

Subscriber private signature keys may be backed up or copied but must be held in the Subscriber's exclusive control. Keys generated for roaming certificates shall be stored in encrypted form on the directory operated by the CA, accessible only by the Subscriber utilizing the Subscriber's activation data.

Private signature keys shall not be escrowed or archived.

7.3.4 Method of Activating Private Key

Private keys will be activated by authenticating the Subscriber to the cryptographic module. Acceptable means of authentication include pass-phrases, PINS, and biometrics.

7.3.5 Method of Deactivating Private Key

Keys will be deactivated as part of the Public Key logout process.

7.4 OTHER ASPECTS OF KEY PAIR MANAGEMENT

7.4.1 Validity Periods for Public and Private Keys

The CA's private signing key used to create certificates will be valid for 20 years. All CA keys (private and public) will be retained in archive in accordance with the procedures in the CPS.

For RAs, LRAs and Subscribers, a private signing key shall be valid for up to 2 years, and certificates issued for the public signature verification key shall be valid for no more than the period required for retention in archive in accordance with the procedures in the CPS.

7.5 ACTIVATION DATA

Inactive RA, LRA and Subscriber private keys will be protected from unauthorized use by encryption keyed with either a password or token.

7.5.1 Password Expiration

Passwords for RAs and LRAs shall expire after 5 weeks. Passwords for Subscribers will expire after 52 weeks. The user must create a new password on the first login after expiration.

7.6 COMPUTER SECURITY CONTROLS

The CA host computer will include the following functionality either provided by the operating system, or through a combination of operating system, CA application, and physical safeguards:

- Access control to CA services and roles;
- CA workstation is physically secured;
- Access to the Entrust/Authority database and audit trails is restricted;
- Enforced separation of duties for CA roles;
- Identification and authentication of CA roles and associated identities;
- Object re-use for CA random access memory;
- Use of cryptography for session communication and database security;
- Key management plan integral to CA design;
- Archival of CA and history and audit data;
- Audit of security related events;
- Self-test of security related CA services;
- Trusted path for identification of CA roles and associated identities; and
- Recovery mechanisms for keys and the CA application.

This functionality is active and logged in the appropriate logs.

7.7 NETWORK SECURITY CONTROLS

The CA application and Repository shall be protected through use of a firewall configured to allow only the protocols and commands required for CA services.

7.8 OFF-SITE BACKUP

- Complete system backups will be taken weekly.
- Weekly backups will be kept for three months and will be stored securely on site.
- Each month one set of backup tapes will be taken to the off site vault.
- Each quarter a complete system backup will be taken to the off-site storage location in St. Louis. (This interval is subject to change as system demands grow)

- Audit logs will be removed from the system as space requirements dictate or at least once every six months. These logs will be backed up on special tapes and archived.
- Other system backups will be taken before and after any major system changes.

8. CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES

8.1 CERTIFICATE PROFILE

All Certificates will be issued in the *X.509 version 3* format and will include the State Policy identifier within the *Certificate Policies* field. The Certificate profiles for Certificates authorized by the State are set forth in this Policy.

8.1.1 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various Certificate Authorities and communities. This Policy shall follow *Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile*, except as modified by the CPS. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be interoperable in their intended community of use.

8.1.2 Algorithm Object Identifiers

Certificates under this Policy will use the following OIDs for signatures:

- ID-DSA-WITH-SHA1 - {ISO(1) MEMBER-BODY(2) US(840) X9-57(10040) X9CM(4) 3}
- sha-1WithRSAEncryption - iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Certificates under this Policy will use the following OIDs for identifying the algorithm for which the subject key was generated:

- id-dsa – {iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
- RsaEncryption- {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
- Dhpublicnumber- {iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
- id-keyExchangeAlgorithm- {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

8.2 CERTIFICATE REVOCATION LIST PROFILE

CRLs will be issued in the X.509 version 2 format. The CRL profile for CRLs issued pursuant to this Policy is as discussed in 8.1.

9. POLICY CHANGE PROCEDURES

9.1.1 Notice

Subscribers and Relying Parties shall periodically check the State Repository for notice of intended modifications to this Certificate Policy document.

9.1.2 Comment Period

Changes to items within this Policy that in the judgment of the Policy Authority will have no/minimal impact on the users using Certificates and Certificate Revocation Lists issued by this Certificate Authority may be made with no change to the Policy version number and no notification to the users.

Changes to the Certificate Policy which, in the judgment of the Policy Authority may have significant impact on the users using Certificates and Certificate Revocation Lists issued by this Certificate Authority, shall undergo a review and comment period of 60 days. The State Policy Authority will review all comments and respond individually or with further changes as appropriate. If the Policy Authority decides not to make any further changes after the 60 day review period the initially-proposed modified document will be published in the Repository.

9.2 PUBLICATION AND NOTIFICATION POLICIES

A copy of this Policy is available in electronic format from the State. Suggested changes may be submitted to the contact person specified in section 3.4 of this CP.

9.3 APPLICABILITY AND ACCEPTANCE OF CHANGES

In order to allow entities to modify their procedures as needed, all changes to this Policy shall become effective 30 days after final publication on the State Repository. It shall be the responsibility of Subscribers and Relying Parties to periodically check the Repository for notice of final publication of this Policy.

Use of or reliance on a Certificate after the 30-day period (regardless of when the Certificate was issued) shall be deemed acceptance of the modified terms.

9.4 POLICY APPROVAL PROCEDURES

The State PA approves this Policy and any subsequent changes.